Claims

1. A computer-implemented method for detecting a macro virus in code adapted for use on a digital computer, said method comprising the steps of:

analyzing the code to determine whether said code contains instructions causing a macro to be moved to a global environment;

when the code contains instructions causing a macro to be moved to a global environment, flagging said macro;

analyzing the code to determine whether said code contains instructions causing the flagged macro to be copied to a local document; and

when the code contains instructions causing the flagged macro to be copied to a local document, declaring that said flagged macro contains a macro virus.

2. The method of claim 1 wherein the macro is contained within a module.

3. The method of claim 1 wherein the code is associated with a Microsoft Excel spreadsheet application.

4. The method of claim 1 wherein the code is written in the Visual Basic language.

5. The method of claim 4 wherein the step of analyzing the code to determine whether said code contains instructions causing a

macro to be moved to a global environment comprises determining whether a SaveAs command is present in the code.

6. The method of claim 4 wherein the step of analyzing the code to determine whether said code contains instructions causing the flagged macro to be copied to a local document comprises determining whether a Copy command is present in the code.

7. The method of claim 1 wherein each analyzing step concatenates strings when said analyzing step encounters a concatenation operator within the code.

8. The method of claim 1 wherein each analyzing step makes substitutions for variable names when the code contains variable names that are proxied.

9. The method of claim 1 wherein each analyzing step traces the values of parameter variables when the code contains instructions that are invoked by other code.

10. The method of claim 1 wherein each analyzing step substitutes object names when the code is written in an object oriented programming language and when the code contains substituted object names.

11. The method of claim 1 further comprising the step of deleting the macro virus.

12. The method of claim 1 wherein publicly identified and publicly unidentified macro viruses are detected.

13. A method for detecting publicly identified and publicly unidentified macro viruses in code adapted for use on a digital computer, said method comprising the steps of:

analyzing the code to determine whether said code contains instructions causing a macro to be moved to a global environment;

when the code does not contain instructions causing a macro to be moved to a global environment, declaring that no macro virus is present;

when the code contains instructions causing a macro to be moved to a global environment, flagging said macro;

analyzing the code to determine whether said code contains instructions causing the flagged macro to be copied to a local document;

when the code does not contain instructions causing the flagged macro to be copied to a local document, declaring that no macro virus is present; and

when the code contains instructions causing the flagged macro to be copied to a local document, declaring that said flagged macro contains a macro virus.

14. Apparatus for detecting publicly identified and publicly unidentified macro viruses, said apparatus comprising:

a digital computer having at least one storage device;

associated with said digital computer, code containing computer instructions;

an application program associated with said computer;

a global environment associated with said application program;

at least one local document generated by said application program and located within said storage device; and

a detection module coupled to said code, said detection module analyzing said code and making the determination that a macro virus is present when said code contains instructions causing a macro to be moved to a global environment and said code also contains instructions causing the same macro to be copied to a local document.

15. The apparatus of claim 14 further comprising a repair module coupled to the detection module and to the code, said repair module adapted to delete the code when the detection module determines that the code contains a macro virus.

16. A computer readable medium containing a computer program for detecting a macro virus in code adapted for use on a digital computer, said program containing instructions for performing the steps of:

analyzing the code to determine whether said code contains instructions causing a macro to be moved to a global environment;

when the code contains instructions causing a macro to be moved to a global environment, flagging said macro;

analyzing the code to determine whether the code contains instructions causing the flagged macro to be copied to a local document; and

when the code contains instructions causing the flagged macro to be copied to a local document, declaring that said flagged macro contains a macro virus.